Códigos de conducta, certificaciones y transferencias internacionales

PID_00250223

Antoni Roig

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Antoni Roig

Índice

1. Códigos de conducta

1) Función y ámbito de aplicación

Un medio para facilitar –a la vez que garantizar– el cumplimiento de las obligaciones del RGPD son los códigos de conducta (arts. 40 y 41 RGPD). Dado que no tenemos una definición de código de conducta en el RGPD, puede ser útil adaptar la definición de la Directiva 2005/29/CE: acuerdo de buenas prácticas no impuesto por las disposiciones legales, reglamentarias o administrativas de un Estado miembro ni por el Derecho de la Unión, pero sí aprobado por la autoridad pública de control competente, el Comité o la Comisión, que contiene buenas prácticas para los responsables y encargados del tratamiento que se adhieran al mismo[1].

(1)Adaptado a partir del art. 2f) de la Directiva 2005/29/CE, de 11 de mayo del 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior. Seguimos, en este punto, a Díaz-Romeral (2016, págs. 389-412).

Como veremos, los códigos de conducta son de utilidad también en las transferencias internacionales de datos. La experiencia de la aplicación de la LOPD y del reglamento LOPD, con los denominados códigos tipo, puede ser muy útil en la aplicación de los arts. 40 y 41 del RGPD (art. 32 de la LOPD y arts. 71 a 78 del Reglamento LOPD). De acuerdo con la disposición transitoria segunda, los promotores de los códigos tipo deberán adaptar su contenido al art. 40 RGPD en el plazo de un año desde la entrada en vigor de la nueva LOPD. De no ser así, se cancelará la inscripción. Su carácter voluntario hace que solo obliguen en la medida en que alguien se someta a ellos[2]. Pueden elaborar códigos de conducta las asociaciones y otros organismos representativos de categorías de responsables (art. 40.2 RGPD), empresas y grupos de empresas, así como responsables y encargados de las instituciones públicas del art. 77.1 APLOPD. Los organismos de supervisión y resolución extrajudicial de conflictos (art. 41 RGPD) podrán promover códigos de conducta. Estos organismos resolverán las reclamaciones denegadas por los responsables (art. 39.3 APLOPD). Su decisión podrá, entonces, trasladarse a la AEPD o a las autoridades autonómicas de protección de datos. Incluso los responsables o encargados no sujetos al RGPD pueden adherirse, para garantizar las transferencias internacionales (arts. 40.3 y 46.2e RGPD). En este caso, los responsables y encargados asumirán compromisos vinculantes y exigibles, mediante contrato u otro instrumento vinculante. Su ámbito de aplicación puede ser nacional, o afectar a varios estados de la Unión Europea[3].

(2)Se trata de un supuesto de autorregulación o, quizá mejor, de corregulación, que sirve para demostrar el cumplimiento de las obligaciones impuestas por el RGPD y, a la vez, para facilitar y especificar la aplicación en ciertos sectores.

(3)La Directiva 95/46/CE, en su art. 27.3, también contemplaba la posibilidad de códigos de conducta de ámbito europeo. Los mismos podían ser sometidos a dictamen del grupo de trabajo del artículo 29, aunque han sido pocos los códigos que han obtenido reconocimiento comunitario: Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización directa (Dictamen favorable del 2003, WP77); y posterior anexo al mismo código (Dictamen 4/2010, WP174). Más recientemente, el Código de conducta sobre proveedores de servicios en la nube (Dictamen 2/2015, WP 232).

Lecturas recomendadas

Sobre el art. 32 de la LOPD y los arts. 71 a 78 del Reglamento LOPD, podéis consultar los trabajos siguientes:

J. Rubí (2009). «Códigos tipo». En: R. Martínez (coord.). *Protección de datos. Comentarios al Reglamento de desarrollo de la LOPD* (págs. 167-199). Valencia: Tirant lo Blanch.

V. Cazurro (2010). «Objeto y naturaleza de los códigos tipo». En: A. Troncoso (dir.). *Comentario a la Ley orgánica de protección de datos de carácter personal* (págs. 1747-1766). Cizur Menor: Civitas-Thomson Reuters.

Y sobre la autorregulación, podéis ver:

S. Rodotà (2010). «Códigos de conducta: entre hard law y soft law». En: A. Real (coord.). *Códigos de conducta y actividad económica: una perspectiva jurídica*. Madrid: Marcial Pons.

2) Procedimiento de elaboración

En el procedimiento de elaboración se consultará a las partes interesadas, incluidos los interesados, si fuera posible[4]. Las asociaciones y otros organismos que agrupen a responsables y quieran elaborar un código de conducta, o modificar uno existente, presentarán el proyecto de código a la autoridad de control competente según el art. 55 RGPD. Esta autoridad –AEPD o autoridad autonómica de protección de datos competente (art. 39.4 APLOPD)–, dictaminará si el proyecto es conforme al RGPD y, si considera que ofrece garantías suficientes, lo aprobará. Si el alcance del código de conducta es nacional, la autoridad de protección de datos registrará y publicará el código. Una vez declarado conforme al RGPD y valorada la suficiencia de sus garantías, el código estará formalmente aprobado y producirá los efectos previstos en el RGPD (Díaz-Romeral, 2016, pág. 401).

(4)El carácter participativo del procedimiento se puede confirmar en el considerando 99 del RGPD.

Si, en cambio, se trata de un código cuyo alcance excede al marco nacional y que afecta a varios estados miembros, la autoridad de protección de datos competente, de acuerdo con el art. 55 RGPD, lo presentará al Comité Europeo de Protección de Datos para que dictamine si ofrece garantías suficientes (art. 40.7 RGPD). De ser así, el Comité presentará su dictamen a la Comisión. En caso contrario, se podría iniciar un diálogo que podría culminar en la presentación, por parte de la autoridad de control competente, de un proyecto de decisión modificado[5] (art. 64.7 RGPD). Finalmente, la Comisión podrá, mediante un acto de ejecución, dar validez general al código de conducta dentro de la Unión Europea. Además, la Comisión dará publicidad a estos códigos dotados de validez general. Finalmente, el Comité archivará todos los códigos aprobados en un registro de acceso público. La AEPD y las autoridades autonómicas de protección de datos mantendrán también un registro accesible por medios electrónicos de los códigos de conducta aprobados por las mismas, así como de los aprobados conforme al art. 63 RGPD.

(5)La autoridad de control también podría mantener su proyecto inicial y forzar la imposición de una decisión vinculante, de acuerdo con el art. 65 RGPD.

3) Contenido

El código de conducta aplica el RGPP y, por ello, son de aplicación los principios y derechos contemplados en el mismo, que deberán concretarse (art. 40 RGPD y también AEPD, 2016):

- El tratamiento leal y transparente.
- El interés legítimo de los responsables.

- La recogida de datos personales.
- La seudonimización de los datos personales.
- La información proporcionada al público y a los interesados.
- El ejercicio de los derechos de los interesados.
- La información proporcionada a los niños y cómo obtener, en este caso, el consentimiento de los padres o tutores legales.
- La responsabilidad, la privacidad por diseño o por defecto y las medidas de seguridad.
- La notificación de las violaciones de seguridad.
- Las transferencias internacionales.
- Los procedimientos de resolución de conflictos, sin perjuicio de las actuaciones de las autoridades de protección de datos y de los tribunales.
- Los procedimientos de control de los incumplimientos, sin perjuicio de las competencias de las autoridades de protección de datos.

En teoría, el contenido es facultativo y, por consiguiente, podrían no estar presentes todos los puntos del art. 40. 2a-k RGPD. Sin embargo, el contenido deberá también ser el adecuado para dar respuesta a la naturaleza del tratamiento, así como los riesgos asociados al mismo. En cualquier caso, la autoridad de control que aprueba el código de conducta deberá valorar la suficiencia de las garantías ofrecidas. Pues bien, pese a su carácter voluntario, será difícil valorar con solvencia las garantías si no se desarrollan los puntos mencionados (Díaz-Romeral, 2016, pág. 400).

4) Supervisión y acreditación

El control sobre el cumplimiento del código lo llevará a cabo un organismo con el nivel técnico suficiente y que, además, haya sido acreditado por la autoridad de protección de datos competente (art. 41 RGPD). Este organismo podrá adoptar medidas de suspensión o incluso la exclusión del infractor del código, siempre respetando unas garantías adecuadas de audiencia y contradicción. Además, se informará de las sanciones adoptadas a la autoridad de protección de datos competente. Todas las actuaciones del organismo de supervisión deberán ser llevadas a cabo en estrecha colaboración con la autoridad de control.

Las autoridades de protección de datos fijarán los criterios de acreditación de un organismo, y someterán el proyecto de criterios al CEPD para su dictamen, a través del mecanismo de coherencia (art. 63 RGPD). Los criterios que la autoridad de control usará para acreditar favorablemente un organismo serán los siguientes:

- Independencia y capacidad técnica adecuada al cometido.
- Adopción de procedimientos de evaluación del cumplimiento del código y revisiones periódicas.
- Adopción de procedimientos transparentes para tramitar las reclamaciones por infracción del código de conducta o sobre cómo se aplica.
- Probar la falta de conflictos de intereses.

Las acreditaciones podrán revocarse si se incumplen estas condiciones, o dejan de cumplirse, o bien si la actuación del organismo incumple el RGPD. También podrá entonces valorar la posibilidad de sancionar hasta con 10 millones de euros al organismo de supervisión del código, por incumplimiento de sus obligaciones derivadas del art. 41.4 RGPD[6] (art. 83.4c RGPD).

[6]Por cierto, en la versión española este precepto se ha traducido incorrectamente como «autoridad de control».

5) Efectos

Seis serían los principales efectos de los códigos de conducta (Díaz-Romeral, 2016, págs. 406-407):

- La clarificación y orientación para cumplir el RGPD.
- El indicio de cumplimiento.
- La consideración de circunstancia atenuante o agravante de la responsabilidad administrativa.
- La obligación de tenerlo en cuenta en la evaluación de impacto.
- La posibilidad de cobertura a una transferencia internacional de datos.
- La confianza y seguridad jurídica.

Una de las virtudes principales del código de conducta es su capacidad para demostrar el cumplimiento de las obligaciones por parte del responsable[7]. Asimismo, permite demostrar el cumplimiento sobre medidas de seguridad[8]. El código de conducta también permite acreditar que se ofrecen garantías suficientes para la transferencia internacional de datos. Se tendrá en cuenta en la evaluación de impacto sobre la protección de datos, así como a la hora de imponer sanciones. Por otro lado, la adhesión a un código permite demostrar la suficiencia técnica del encargado o subencargado[9]. Se trata, pues, de un principio de prueba de cumplimiento, que la autoridad de control debe tener en cuenta a la hora de imponer una multa administrativa. Es decir, un responsable o encargado que se haya venido ajustando a lo previsto en el código de conducta debería ver su responsabilidad atenuada. En cambio, la simple adhesión a un código de conducta no supondría este efecto positivo. Incluso podría llegar a agravarse la responsabilidad si se incumpliera reiteradamente, aprovechando la confianza generada de manera ilegítima en los interesados[10] (Díaz-Romeral, 2016, pág. 398).

(7)Así, el considerando 148 incluye la adhesión a códigos de conducta entre las circunstancias agravantes o atenuantes de la responsabilidad administrativa. Por otro lado, en el art. 24.2 RGPD se afirma expresamente que la adhesión a un código de conducta o a un mecanismo de certificación podrá ser utilizada para demostrar el cumplimiento de las obligaciones del responsable.

(8)El art. 32.3 RGPD, en efecto, prevé que la adhesión a un código de conducta permita acreditar que el responsable y el encargado aplican las medidas de seguridad, técnicas y organizativas, adecuadas al riesgo para los derechos del interesado.

(9)De acuerdo con el art. 28.5 RGPD, la adhesión del encargado del tratamiento a un código de conducta podrá acreditar la existencia de las garantías suficientes que se exigen en el artículo.

(10)Díaz-Romeral sostiene, además, que la falta de supervisión debida, de acuerdo con el art. 41.4 RGPD, podría ser sancionable conforme al art. 83.4c RGPD.

Los actuales códigos tipo inscritos en el Registro General de Protección de Datos deberán modificarse y adaptarse al RGPD[11]. En Estados Unidos, los códigos de conducta que actualmente se basan en los FIPP (*fair information practice principles*) deberán, igualmente, tener en cuenta las modificaciones introducidas por el RGPD[12]. De hecho, en los dictámenes más recientes del grupo del artículo 29 sobre códigos de conducta, de acuerdo con el artículo 30 de la Directiva 95/46/CE, se tiene en cuenta también el que se ha convertido en el Reglamento 2016/679. Así, en la opinión 02/2015 sobre el Código de conducta sobre *cloud computing* de C-SIG, el enfoque está orientado también al cumplimiento del RGPD[13]. Se trata, así, de un primer anticipo de lo que pueden ser futuras opiniones sobre códigos de conducta después de mayo del 2018. Un aspecto inicial relevante es el hecho de que la adhesión al código, aunque sea anterior al 2018, no excluirá la aplicación del RGPD cuando este sea de aplicación a partir de mayo del 2018, ni impedirá las sanciones de las autoridades de protección de datos. Pese a esto, se recomienda la adopción de códigos de conducta para ayudar a demostrar, precisamente, el cumplimiento del RGPD. Un aspecto criticado es la necesidad de que el código especifique la localización del procesamiento, es decir, dónde tiene lugar el mismo, a efectos de poder identificar la ley aplicable e informar al interesado si algún dato es enviado fuera de la Unión Europea. El responsable y la autoridad de control deberían, así, poder tener indicaciones de localidades de procesamiento de datos.

(11)Decisión de la Comisión de 27 de diciembre del 2001, sobre cláusulas contractuales estándar para la transferencia de datos personales a encargados establecidos en países terceros, de acuerdo con la Directiva 95/46/CE.

(12)Por ejemplo, la *Network Advertising Initiative (NAI) ha adoptado un Código de conducta para la industria de la publicidad en línea.*

(13)Opinión 02/2015 sobre el Código de conducta de C-SIG sobre *cloud computing*, adoptado el 22 de septiembre del 2015.

Lectura recomendada

Al respecto de la adopción de un código de conducta para la industria de la publicidad en línea, podéis ver el artículo siguiente:

A. Myers (2016). «Cross-Border Commerce without constraint: Shifting from Territorial-Based Regulation to an Industry-Based Code of Conduct for the Online Payment Processing Industry». *The Computer & Internet Lawyer* (vol. 33, núm. 7, págs. 11-24).

Por otro lado, se recuerda que la noción de dato personal debe ser respetada, incluso en el caso de seudónimos que, como sabemos, no excluyen la aplicación de la normativa de protección de datos. En cuanto a la transferencia internacional de datos, de acuerdo con el nuevo art. 43 RGPD, el encargado debería comunicar al responsable cualquier puesta a disposición de datos personales, a requerimiento de autoridades públicas ejecutivas, salvo prohibición legal expresa. En todo caso, el envío de estos datos personales a autoridades públicas no puede ser masivo, desproporcionado e indiscriminado, pues esto no es necesario en una sociedad democrática. Otro aspecto criticado es la falta de claridad de la asignación de responsabilidades entre responsable y encargado, y la consiguiente falta de información al interesado sobre este punto, así como la falta de previsión de mecanismos de reclamación. Por otro lado, las medidas de seguridad no están suficientemente adaptadas a los diferentes niveles de protección necesaria, según el tipo de dato y de tratamiento. Finalmente, se aconseja incluir una mención al derecho a la portabilidad de los datos.

2. Certificaciones, sellos y marcas de protección de datos

1) Definición y funciones

La certificación es «la acción llevada a cabo por una entidad independiente de las partes interesadas mediante la que se manifiesta que una organización, producto, proceso o servicio, cumple con los requisitos definidos en una norma o especificaciones técnicas» (AENOR). En definitiva, se trata de un mecanismo para aumentar la transparencia y el cumplimiento del RGPD (considerando 100 del RGPD). En efecto, las certificaciones, los sellos y las marcas de protección de datos cumplen una función de acreditación del cumplimiento del RGPD por parte de los responsables y encargados[14] (Fernández y Recio, 2016). Por otro lado, sirven para justificar que se proveen garantías adecuadas para las transferencias internacionales de datos. En este caso, los responsables y encargados de los terceros países deberán asumir compromisos vinculantes y exigibles, por ejemplo, mediante un contrato. Finalmente, permiten evaluar más fácilmente el nivel de protección de datos ofrecido. Al igual que sucede con los códigos de conducta, las certificaciones son voluntarias y deberán estar disponibles a través de un proceso transparente (art. 42.3 RGPD). Debido a todas estas ventajas, los estados, las autoridades de protección de datos y el CEPD impulsarán la adopción de estas certificaciones, teniendo en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

(14)La Directiva 95/46/CE no hacía referencia, en cambio, a la certificación ni a otros distintivos como los sellos o marcas de protección de datos. La AEPD, en su Plan estratégico 2015-2019, contempla la certificación, la acreditación y la auditoría en su eje estratégico 1, de prevención para una protección más eficaz. Reglamento (CE) 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio del 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos.

Ahora bien, pese a su capacidad para acreditar el cumplimiento, la existencia de una certificación no excluye el deber general de cumplimiento del RGPD por parte de los responsables y encargados. Por esta razón, las certificaciones no impiden la fiscalización de las autoridades de protección de datos, ni exoneran de las eventuales sanciones que pudieran imponerse a los responsables. Por consiguiente, las certificaciones no limitarán la responsabilidad del responsable o encargado. Este aspecto ha sido criticado por representantes empresariales que creen que esto resta eficacia, y hasta razón de ser, a las certificaciones[15].

(15)Quizá, la referencia a los responsables y encargados no sujetos al presente Reglamento del art. 42.2 RGPD pudiera haberse ampliado sin más a los responsables y encargados sujetos al mismo, como sugieren Fernández y Recio (2016, pág. 418).

Las funciones de las autoridades de control en relación con la certificación pueden resumirse como sigue (Fernández y Recio, 2016, págs. 423-424):

- Fomentar la creación de mecanismos de certificación (art. 57.1n RGPD).
- Aprobar los criterios de certificación (art. 57.1n RGPD y art. 58.3f RGPD).

- Revisar periódicamente las certificaciones (art. 57.1o RGPD).
- Elaborar y publicar los criterios de acreditación (art. 57.1p RGPD).
- Acreditar los organismos de certificación (art. 57.1q RGPD y art. 58.3e RGPD).
- Expedir y revisar las certificaciones expedidas (art. 58.1c RGPD y art. 58.3 f RGPD).
- Retirar u ordenar la retirada o no emisión de una certificación (art. 58.2h RGPD).

2) Procedimiento

El certificado lo puede expedir un organismo acreditado, una autoridad de protección de datos competente o el CEPD[16]. Esto supone que la autoridad de protección de datos aprobará unos criterios de certificación. En un ámbito europeo, el CEPD aprobará una certificación común: el sello europeo de protección de datos. El organismo certificador podrá recabar del responsable y encargado toda la información necesaria para llevar a cabo la certificación. Por consiguiente, los responsables o encargados deberán facilitar el acceso a sus actividades de tratamiento por parte del organismo de certificación.

(16)En el *Statement on the 2016 action plan for the implementation of the general Data Protecion Regulation* (GDPR), adoptado el 2 de febrero del 2016, se indica que el WP29 adoptará una guía sobre certificaciones (WP236).

La certificación tendrá una validez temporal limitada de un máximo de tres años, y podrá renovarse en las mismas condiciones, siempre que se sigan cumpliendo los requisitos[17]. El organismo certificador deberá comunicar previamente a la autoridad de protección de datos su intención de certificar o renovar la certificación existente. La autoridad de protección de datos podrá retirar la certificación u ordenar que no se expida, en caso de que no se cumplan los requisitos de certificación.

(17)Se ha criticado que el plazo de tres años podría ser excesivamente largo, dada la rapidez del cambio tecnológico. Esto podría tener como consecuencia una mala práctica, consistente en concentrar los esfuerzos para cumplir el RGPD justo antes de la renovación de la certificación, y luego no hacer un esfuerzo continuado en su observancia (Carpio, 2016, pág. 344).

3) Organismos de certificación acreditados

Como hemos dicho anteriormente, no solo la autoridad de protección de datos o el CEPD podrán certificar, sino también los organismos debidamente acreditados (art. 42.5 RGPD). Pues bien, los organismos de acreditación serán estos mismos, junto con el organismo nacional de acreditación, de acuerdo con el Reglamento (CE) 765/2008 y las normas EN ISO/IEC 17065/2012 y UNE-ISO/IEC 17065, y siguiendo los requisitos establecidos por la autoridad de protección de datos[18]. Por consiguiente, si quien acredita es una autoridad de control, se deberán considerar los criterios establecidos por la misma o por el Comité Europeo, mientras que, si se trata de un organismo nacional de acreditación, deberán complementarse a los mismos los del Reglamento (CE) 765/2008 y las normas técnicas de métodos y procedimientos. En España, el organismo nacional de acreditación es la ENAC (Entidad Nacional de Acreditación)[19], que

(18)UNE-ISO/IEC 17021-1:2015. *Evaluación de la conformidad - Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión - Parte 1: Requisitos*; UNE-EN ISO/IEC 17065:2012. *Evaluación de la Conformidad. Requisitos para organismos que certifican productos, procesos y servicios*. ISO/IEC 27006:2015. *Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems*.

comunicará a la AEPD y a las autoridades autonómicas de protección de datos las concesiones, denegaciones o revocaciones de las acreditaciones (art. 40 APLOPD).

(19)Real Decreto 1715/2010, de 17 de diciembre, por el que se designa a la Entidad Nacional de Acreditación (ENAC) como organismo nacional de acreditación, de acuerdo con lo establecido en el Reglamento (CE) 765/2008. Al ser considerado en el Real Decreto como el «único» organismo nacional de acreditación, se planteó un conflicto positivo de competencias por parte de la Generalitat de Cataluña, resuelto finalmente en favor de la Administración general en la STC 20/2014, de 10 de febrero.

Las autoridades de protección de datos harán públicos los criterios y requisitos para la acreditación, y se comunicarán al Comité Europeo. Aunque estamos todavía pendientes de que se concreten, de manera general pueden indicarse los siguientes aspectos clave para la acreditación:

- Mostrar independencia y ausencia de conflicto de interés (arts. 43.2a y 43.2e RGPD).

- Ser transparente y fijar procedimientos para la tramitación, por parte de los responsables y los encargados de las reclamaciones, por infracciones de las certificaciones (art. 42.3 RGPD, en cuanto al proceso de certificación, y art. 43.2d RGPD en cuanto a los procedimientos de reclamación).

- Mostrar pericia en el objeto de certificación (art. 43.2a RGPD).

- Profesionalidad y respeto a los criterios de certificación (art. 43.2b RGPD).

- Establecer procedimientos para la expedición, revisión periódica y retirada de certificados, sellos y marcas (art. 43.2c RGPD).

Criterios de acreditación de la ENAC

Los criterios de acreditación de la ENAC se encuentran en su folleto institucional (pág. 12). De acuerdo con el mismo, el organismo de certificación deberá demostrar lo siguiente:

- Que cuenta con personal cualificado y experimentado.
- Dispone de un equipamiento e infraestructuras adecuados y mantenidos adecuadamente.
- Aplica métodos de evaluación válidos y apropiados.
- Emplea técnicas de control de calidad de resultados.
- Asegura la trazabilidad de las mediciones a patrones internacionales.
- Informa de manera adecuada a los clientes y emite informes o certificados claros.
- Cuenta con un sistema de aseguramiento de la calidad de su gestión.

La acreditación de un organismo de certificación tiene una vigencia de un máximo de cinco años, renovable. Podrá revocarse si la autoridad de protección de datos o la autoridad nacional consideran que se incumplen los requisitos de

la acreditación o el RGPD: es decir, por incumplir las obligaciones de correcta evaluación a efectos de la certificación o retirada de la misma (art. 43.4 RGPD) y de comunicación a las autoridades de control competentes de las razones de la expedición de la certificación solicitada o de su retirada (art. 43.5 RGPD). Esto no exime a los responsables y encargados de su responsabilidad por incumplimiento del RGPD. El Comité Europeo gestionará un registro público de los certificados, sellos y marcas, los organismos acreditados, y responsables y encargados certificados y establecidos en terceros países, cuando sirvan de garantía para las transferencias internacionales de datos. Se prevén sanciones por incumplimiento de las obligaciones, que pueden llegar hasta los 10 millones de euros. La Comisión podrá adoptar actos delegados o ejecutivos para especificar las condiciones de los mecanismos de certificación, previo dictamen del CEPD. Asimismo, la Comisión podrá adoptar normas técnicas para promover y reconocer los certificados, sellos y marcas.

4) Efectos

La certificación, los sellos y las marcas podrán demostrar el cumplimiento de las obligaciones del responsable, en general. Concretamente, pueden certificar el uso de la privacidad por diseño y por defecto, la adopción de medidas de seguridad adecuadas, la suficiencia técnica de los encargados y subencargados y las garantías suficientes para la transferencia internacional de datos. Otro aspecto destacable es que serán tenidas en cuenta a la hora de aplicar las sanciones. Como hemos dicho anteriormente, la certificación no excluye la responsabilidad por incumplimiento del RGPD. Queda por ver si los responsables se acogerán a esta posibilidad, y en qué medida. Dependerá, en buena parte, de lo estricta que sea la aplicación de sanciones por incumplimiento del RGPD a empresas que, en cambio, estén certificadas.

3. Transferencias internacionales de datos personales

3.1. Decisión de la Comisión sobre el nivel adecuado de protección

El RGPD dedica especial atención a las transferencias internacionales de datos personales[20] (Remolina, 2015; Piñar, 2016). Pese a no contener una definición de transferencia internacional, ni de tercer país, las comunicaciones de datos entre miembros de la Unión no se consideran transferencias internacionales[21]. Las transferencias internacionales se refieren a países no comunitarios o a organizaciones internacionales[22]. El concepto de transferencia internacional parece incluir no solo el envío de información, sino también la puesta a disposición de los datos para su consulta[23]. El régimen de transferencia internacional de datos es aplicable no solo a los responsables, sino también a los encargados (art. 44 RGPD).

Ved también

Las transferencias internacionales de datos serán estudiadas de forma más detallada en la asignatura *Requisitos legales en el procedimiento de tratamiento de los datos personales II*.

(20)Capítulo V del RGPD, arts. 44 a 50 y considerandos 101-116. En comparación, la Directiva 95/46/CE dedicaba únicamente los arts. 25 y 26 y los considerandos 56 a 60 a las transferencias internacionales de datos personales. Esta regulación desplazará en buena medida la LOPD, arts. 33 y 34, y el Reglamento LOPD, arts. 65-70 y 137-144. La importancia de las transferencias internacionales de datos también es manifiesta en el considerando 101 del RGPD y, por ello, la necesidad de preservar también en estos casos los derechos de los interesados obliga a una regulación detallada.

(21)La Directiva 95/46/CE tampoco contenía ninguna definición de transferencia internacional.

(22)El Reglamento LOPD se refiere, en este sentido, a las transferencias fuera del espacio económico europeo. Sin embargo, el RGPD parece considerar a los países del EEE como terceros, y también se deberá resolver la nueva situación del Reino Unido.

(23)Así, el art. 49.1g RGPD considera válida una transferencia cuando se lleve a cabo desde un registro público que, de acuerdo con el Derecho europeo o nacional, tenga como objeto facilitar información al público en general o a cualquier persona que acredite interés legítimo, siempre que se cumplan las condiciones del Derecho de la Unión para la consulta.

La Comisión Europea puede considerar que un país tercero garantiza un nivel adecuado de protección, atendiendo al marco regulador de su Estado de Derecho y a la protección de los derechos fundamentales[24]. Se tiene en cuenta, en este sentido, la legislación de seguridad pública, defensa y seguridad nacional, legislación penal, y la posibilidad de acceso a una autoridad de protección de datos y la aplicación de la normativa de protección de datos. También se valoran la jurisprudencia y los derechos protegidos, mediante recursos administrativos y acciones judiciales[25] (art. 45.2a RGPD).

(24)El art. 45 RGPD recoge lo que era el modelo central en la Directiva 95/46/CE, aunque ahora se atribuye la decisión únicamente a la Comisión Europea, y no así a los estados miembros (considerando 103). El considerando 102 del RGPD se refiere también a los acuerdos internacionales suscritos por la Unión Europea o por los estados miembros. Esta previsión no se ha incluido en el articulado del RGPD, salvo lo previsto en el art. 96 RGPD. En lo concerniente a los acuerdos internacionales ya suscritos por la Unión, deberán respetar, cuando menos, la Directiva 95/46/CE, y seguirán en vigor hasta que sean modificados. A partir del 25 de mayo del 2018, los nuevos acuerdos tendrán que respetar ya el RGPD.

(25)Tiene especial relevancia la adhesión al Convenio 108 del Consejo de Europa, como quedó demostrado en el reconocimiento de la adecuación de Uruguay (Piñar, 2016, pág. 443, nota 30).

Otro aspecto relevante que hay que tener en cuenta es la existencia de autoridades de protección de datos que sean independientes, con capacidad de fiscalización del cumplimiento de la normativa, poder sancionador, y que cooperen con las autoridades de protección de datos de la Unión Europea o de algún Estado miembro. Se valorará, igualmente, que el Estado haya asumido compromisos internacionales multilaterales o regionales sobre protección de datos.

Una vez que haya evaluado la adecuación del nivel de protección de un país tercero, la Comisión Europea podrá adoptar mediante un acto delegado o ejecutivo un mecanismo de revisión periódico de la evaluación, al menos cada cuatro años. El acto de ejecución indicará su ámbito de aplicación y determinará la autoridad de control competente. Además, la Comisión tendrá que consultar al CEPD y supervisar y evaluar su aplicación, informando al CEPD y al Parlamento Europeo[26]. Cuando la Comisión considere que un país tercero o una organización internacional ya no garantizan un nivel de protección adecuado, podrá derogar, mediante un acto de ejecución, su anterior decisión. Igualmente, la Comisión puede entablar consultas con el país en cuestión, con el fin de reconducir la situación.

(26)Los dictámenes del Comité Europeo son prescriptivos, pero no vinculantes (art. 70.1s RGPD y considerando 105), y puede actuar de oficio o a instancia de la Comisión (art. 70.1 RGPD). Ahora bien, los dictámenes de su antecesor, el grupo de trabajo del art. 29, eran determinantes en la práctica.

La Comisión publicará en el *Diario Oficial de la Unión Europea* y en su página web una lista de terceros países y organizaciones internacionales que, en su opinión, garantizan un nivel de protección adecuado. Las decisiones de adecuación adoptadas de acuerdo con la Directiva 95/46 permanecerán en vigor hasta su sustitución o derogación: Suiza, Argentina, Guernsey, Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y Canadá (ley canadiense *Personal Information and Electronic Documents Act*). El acuerdo Safe Harbour con Estados Unidos ha sido invalidado por el TJUE, y en su lugar se aplicará el *Privacy Shield*[27]. Los principios de privacidad que las empresas americanas deberán cumplir en su autocertificación son el principio de notificación a los interesados, el principio de integridad de los datos y de limitación de la finalidad, el principio de seguridad, el principio de acceso y el principio de recurso, aplicación y responsabilidad. También se aplicarán normas especiales para las «transferencias ulteriores». No será fácil, sin embargo, aplicar la autocertificación y los compromisos de supervisión adoptados por varias administraciones y agencias estadounidenses en el marco del escudo de la privacidad Unión

(27)Decisión de ejecución (UE) 2016/1250 de la Comisión, de 12 de julio del 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el escudo de la privacidad UE-EE. UU.

(28)A partir de la STJUE de 6 de octubre del 2015, caso Schrems, que declara inválida la Decisión sobre el puerto seguro. La Comisión ha aprobado la Decisión de ejecución (UE) 2016/2295, de 16 de diciembre del 2016, donde se reconoce el poder de supervisión de las autoridades de control y se obliga a un seguimiento de la regulación de acceso a los datos personales por parte de las autoridades públicas, en el marco de las decisiones de adecuación.

Europea-Estados Unidos (Reichel, 2017). Las autoridades de control pueden, pese a todo, comprobar si una transferencia llevada a cabo al amparo de una decisión de adecuación respeta o no el RGPD[28].

Lecturas recomendadas

Existe una guía de la Unión Europea sobre el escudo de privacidad, disponible en *Guía del escudo de la privacidad UE-EE UU*, y también puede verse WP29, *Opinion 01/2016 on EU-US Privacy Shield draft adequacy decision*, adoptada el 13 de abril del 2016. Sobre el intercambio de datos personales con EE. UU. para propósitos de cooperación policial, se aplica, en cambio, el *umbrella agreement*, o Acuerdo marco, *Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses* (02-06-2016).

Sobre las dificultades para la supervisión exigida por la Unión Europea a los comités bioéticos y a los órganos de protección de la privacidad en Estados Unidos, véase el artículo de J. Reichel, quien sugiere, en su lugar, una autorregulación y una estandarización supervisada por un órgano nacional de control.

J. Reichel (2017). «Oversight of EU medical data transfers - an administrative law perspective on cross-border biomedical research administration». *Health Technol* (7 de marzo, págs. 1-12).

Las cláusulas estándar o tipo, de carácter voluntario, continuarán en vigor hasta su sustitución por otras adaptadas al RGPD. La AEPD podrá adoptar cláusulas contractuales tipo para llevar a cabo transferencias internacionales de datos que serán sometidos previamente al Comité Europeo de Protección de Datos (art. 42.1 APLOPD). En casos de países sin decisión de adecuación, y que no ofrecían garantías adecuadas, estas cláusulas estándar eran una mejor solución, en opinión del WP29[29], que usar simplemente la habilitación de circunstancias excepcionales del art. 26 de la Directiva 95/46/CE. La Comisión había adoptado distintos tipos de cláusulas estándar, dependiendo de si la transferencia tenía lugar desde un responsable de los datos hacia otro en un país tercero, o desde un responsable a un encargado en un país tercero[30].

[29]WP29, *Working document on a common interpretation of Article 26(1) of Directive 95/46/CE of 24 October 199*, adoptado el 25 de noviembre del 2005 (WP 114). Así, se han adoptado cláusulas estándar para la transferencia a encargados en países que no aseguran un nivel adecuado de protección de los datos personales (Decisión de la Comisión C2010/593) y entre responsables, de acuerdo con la Decisión 2001/497/CE.

[30]Un primer grupo de cláusulas lo encontramos en la Decisión 2001/497/CE, de 15 de junio, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país, previstas en la Directiva 95/46/CE (WP29 WP 38 y WP47); un segundo grupo, en la Decisión 2004/915/CE, de 27 de diciembre, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países (véase también la Decisión de la Comisión C2004/5721), y un tercero, en la Decisión 2002/16/CE, reemplazada luego por la Decisión 2010/87/CE, *On standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (Commission Decision C2010/593)*.

Una perspectiva final que puede cobrar importancia en el futuro son las herramientas técnicas de garantía del cumplimiento del intercambio de datos: por ejemplo, en el caso de los datos médicos, el proyecto europeo BioMedBridges ofrece una herramienta interactiva para garantizar el cumplimiento de los intercambios de datos para fines de investigación (Kuchinke y otros, 2016).

De acuerdo con la disposición adicional quinta del APLOPD, un ciudadano podrá reclamar ante la AEPD una decisión de la Comisión de Adecuación, con audiencia del responsable. Si la AEPD considera que la reclamación está fundada, solicitará de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional autorización para declarar contraria a derecho la transferencia inter-

nacional. Esta autorización requerirá plantear previamente cuestión prejudicial de validez (art. 267 TFUE), y que el TJUE declare inválida la decisión de la Comisión Europea.

3.2. Garantías adecuadas

Si no existe una decisión de adecuación de la Comisión, entonces solo podrán transmitirse datos personales a un tercer país u organización internacional[31] si se ofrecen las garantías adecuadas y los interesados disponen de derechos y acciones legales efectivas (art. 46 RGPD). No se requerirá ninguna autorización expresa de una autoridad de control cuando estas garantías se aporten mediante:

(31)Se trata de una novedad del RGPD. La definición de organización internacional se encuentra en el art. 4.26 RGPD. Su específica mención quiere dar respuesta al hecho de que las organizaciones internacionales se rigen por su tratado internacional constitutivo, y no por el ordenamiento del país donde se encuentren.

- Un instrumento jurídico vinculante y exigible entre autoridades y organismos públicos.

- Normas corporativas vinculantes (*binding corporative rules*, BCR).

- Cláusulas estándar o tipo de la Comisión, o de las autoridades de protección de datos y la Comisión (requiere procedimiento de examen o mecanismo de coherencia, de acuerdo con el art. 63, apartado 2 RGPD).

- Códigos de conducta o certificaciones, junto con compromisos vinculantes y exigibles del responsable o el encargado.

Si existe una autorización por parte de una autoridad de control competente, serán suficientes:

- Contratos específicos entre el exportador y el importador, con autorización de las autoridades de protección (requiere mecanismo de coherencia, art. 63 RGPD).

- Acuerdos administrativos entre autoridades y organismos públicos, con autorización de la autoridad de protección de datos y mecanismo de coherencia.

Las transferencias internacionales o comunicaciones solicitadas por una sentencia judicial o una autoridad administrativa solo serán ejecutivas si se basan en un acuerdo internacional vigente entre el país tercero y la Unión Europea o un Estado miembro y, además, siempre que sea una transferencia legítima[32] (art. 48 RGPD). Los estándares que no provengan de la Comisión o de una autoridad de protección de datos pueden requerir garantías adicionales. Este es el caso, por ejemplo, del estándar *Common Reporting Standard* (CRS) de la OCDE[33] (CRS, aprobado por el Consejo de la OCDE el 15 de julio del 2014). El WP29 reconoce la justificación de interés público de los intercambios automá-

ticos internacionales de datos personales por motivos fiscales[34]. Ahora bien, se afirma igualmente la conveniencia de respetar los principios de protección de datos, concretamente los principios de limitación de propósito y de necesidad.

(32)El RGPD quiere regular, en su art. 48, las exigencias de los procedimientos *pre-trial discovery*, propios de ciertos ordenamientos de *common law*, como el estadounidense. El considerando 115 se refiere a las comunicaciones que no se basen en un acuerdo internacional, y que sean necesarias por razones de interés público reconocido en la Unión o en el Derecho nacional. Al respecto, véase Piñar (2016, págs. 437-438) y también el documento 1/2009 del grupo de trabajo del artículo 29, *Pre-trial Discovery for cross border civil litigation* (WP158). La mejor opción sería aplicar el Convenio de La Haya de 18 de marzo de 1970. Sin embargo, como explica J. L. Piñar, dado que España ha formulado una reserva al artículo 23 del Convenio de La Haya, la cesión es difícilmente admisible (2016, pág. 438, nota 19).

(33)*Standard for Automatic Exchange of Financial Account Information - Common Reporting Standard*.

(34)Decisión del grupo de trabajo del artículo 29 sobre intercambios automáticos entre estados de datos personales para finalidades fiscales, adoptada el 4 de febrero del 2015 (WP230).

Más adelante, el WP29 ha adoptado una guía sobre intercambio automático de datos personales para finalidades fiscales[35]. Al respecto, la guía distingue varias situaciones:

(35)Grupo de trabajo del artículo 29, *Guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purpose*, adoptado el 16 de diciembre del 2015 (WP 234).

a) Intercambio de datos entre estados miembros: las garantías consistirán en aplicar el principio de necesidad y proporcionalidad; la información correcta al interesado sobre los datos que se transferirán y la finalidad; el derecho de acceso y rectificación; la supervisión de una autoridad de control; y la posibilidad de reclamar. Dentro de un mismo Estado, una Administración pública deberá informar a los interesados sobre las transferencias a otras administraciones públicas y su propósito[36].

(36)Caso C-201/14, Smaranda Bara y otros, de 1 de octubre del 2015.

b) Intercambio con un Estado cubierto por una decisión de adecuación: la transferencia requerirá cumplir con las garantías de la decisión de adecuación. La autoridad de control supervisará y evaluará si las garantías ya no son adecuadas[37]. Por consiguiente, las garantías de todos los acuerdos deberán ser evaluadas regularmente.

(37)Caso C-362/14, Schrems contra autoridad de protección de datos, de 6 de octubre del 2015.

c) Intercambio con un Estado no cubierto por una decisión de adecuación. En este caso, siempre deberán incluirse las siguientes garantías: base legal para el tratamiento; finalidad acotada; necesidad y proporcionalidad[38]; periodo de retención de los datos[39]; transparencia y regularidad en el procesamiento; derechos de los interesados; asignación clara de responsabilidades; eventuales transferencias ulteriores; medidas de seguridad y comunicación de violaciones de seguridad; evaluaciones de impacto; y prevención de usos para otras finalidades.

(38)Grupo de trabajo del artículo 29, opinión 01/2014, sobre la aplicación de los conceptos de necesidad y proporcionalidad por parte de las autoridades ejecutivas (WP211).

(39)Casos acumulados C-293/12 y C-594/12, *Digital Rights Ireland*, de 8 de abril del 2014.

Finalmente, se incluyen en la guía algunas cláusulas para eventuales acuerdos de cooperación para finalidades fiscales, y se indican en el anexo unos cuestionarios para los acuerdos bilaterales o multilaterales entre autoridades fiscales.

Se advierte, pese a todo, que en este ámbito es necesaria la aproximación caso por caso, de acuerdo con el contexto concreto del intercambio y los riesgos presentes. La regla de cierre para los supuestos que no cuenten con una decisión de adecuación aprobada por la Comisión, y que no se amparen en una garantía del art. 42 APLOPD o en el art. 46.2 RGPD, es la necesaria y previa autorización por parte de la AEPD y la autoridad autonómica de protección de datos competente (art. 43.1 APLOPD), sometida a dictamen del Comité Europeo de Protección de Datos. Si se alega la necesidad de transferencia internacional para fines relacionados con intereses legítimos, de acuerdo con el art. 49.1 RGPD, deberá informarse, con carácter previo a la realización de la transferencia, a la AEPD o autoridad autonómica de protección de datos competente (art. 44 APLOPD).

3.3. Normas corporativas vinculantes (*binding corporative rules*, BCR)

Las BCR son acuerdos vinculantes reconocidos por la normativa europea de protección de datos, sin necesidad de autorización específica (art. 47 RGPD)[40]. Para poder legitimar la transferencia internacional de datos, deben ser aprobados por la autoridad de protección de datos competente, y requieren el mecanismo de coherencia[41]. Esto solo será posible si las BCR son jurídicamente vinculantes, y todos los miembros del grupo empresarial que suscribe el BCR se encuentran legalmente vinculados a sus contenidos, incluidos los empleados. Además, es necesario que se contemplen expresamente los derechos de los interesados en relación con el tratamiento de sus datos personales. Finalmente, su contenido mínimo deberá ser:

(40) Se trata de una de las novedades más importantes del RGPD. Se puede encontrar una definición de las mismas en el art. 4.20 RGPD.

(41) La AEPD podrá adoptar normas corporativas vinculantes a instancia de una entidad situada en España, mediante un procedimiento cuya duración máxima será de un año, y que se suspenderá hasta obtener el dictamen del Comité Europeo de Protección de Datos (art. 42.2 APLOPD).

- La estructura del grupo empresarial y los datos de contacto de todos sus miembros.

- Las transferencias, las categorías y el tratamiento de los datos, los afectados, los fines y el país tercero en cuestión.

- Carácter jurídicamente vinculante, tanto en un ámbito interno como externo.

- Aplicación de los principios generales de protección de datos: limitación de la finalidad, minimización de los datos, periodos de conservación limitada, calidad de los datos, protección de datos desde el diseño y por defecto, categorías especiales, seguridad y requisitos para las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes.

- Los derechos de los interesados y medios para ejercerlos: derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, derecho a presentar una reclamación ante una autoridad de control

competente y ante los tribunales, y derecho a una reparación o indemnización por violación de las BCR, cuando proceda.

- Aceptación de la responsabilidad por actuación de miembros fuera de la Unión Europea, con exoneración si demuestra que el acto no le es imputable.
- La forma de informar de las BCR a los interesados.
- Las funciones del delegado para la protección de datos.
- Los procedimientos de reclamación.
- Los mecanismos para garantizar la verificación del cumplimiento (auditorías y acciones correctivas).
- Los procedimientos para su modificación y notificación a la autoridad de control.
- Los mecanismos de cooperación e información a las autoridades de control.
- La formación en protección de datos del personal que tenga acceso permanente o habitual a los datos personales.

La Comisión podrá adoptar un acto de ejecución para especificar el formato y los procedimientos de intercambio de información entre responsables, encargados y autoridades de control en relación con las BCR. En el marco de la Directiva 95/46/CE, el WP29 adoptó varios documentos sobre la estructura de las BCR, sobre los requisitos nacionales de las BCR para el responsable[42] (BCR-C, del inglés *controller*) y para el encargado[43]. Igualmente, existe un documento del mismo WP29 sobre las transferencias de datos en la Zona de Cooperación Económica Asia-Pacífico[44] (APEC, en inglés).

[42]WP29, *National filing requirements for controller BRC (BCR-C)*, actualizado en febrero del 2016.

[43]WP29, *Explanatory document on the processor binding corporate rules*, adoptado el 19 de abril del 2013 (WP 204) y revisado el 22 de mayo del 2015 (WP 204 rev.01).

[44]WP29, *Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents*, adoptado el 27 de febrero del 2014.

Legislación sobre la estructura de las BCR

De los documentos que el WP29 adoptó sobre la estructura de las BCR, quizá el de referencia sea el WP 212, de 27 de febrero del 2012. Otros documentos del WP29 son los siguientes:

- *Working Document Setting up a framework for the structure of Binding Corporate Rules*, adoptado el 24 de junio del 2008 (WP 154).
- *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules*, adoptado el 24 de junio del 2008 y revisado y adoptado el 8 de abril del 2009 (WP 155, rev. 04).

- *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, adoptado el 24 de junio del 2008 (WP 153).

Con anterioridad, el WP29 ya había adoptado:

- La *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*, adoptada el 10 de enero del 2007 (WP 133).
- El *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules*, adoptado el 14 de abril del 2005 (WP 108).
- El *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From Binding Corporate Rules*, adoptado el 14 de abril del 2005 (WP 107).
- El *Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, adoptado el 3 de junio del 2003 (WP 74).

3.4. Excepciones

Si falta una decisión de adecuación por parte de la Comisión, y tampoco se ofrecen las garantías adecuadas descritas anteriormente, incluidas las normas corporativas vinculantes, entonces la transferencia solo será posible si se dan las siguientes excepciones para situaciones específicas[45] (49 RGPD) (Piñar, 2016, págs. 454-456):

(45)El grupo de trabajo del art. 29 interpretó en su momento muchas de estas excepciones al Derecho europeo: WP 12, adoptado el 24 de julio de 1998, y WP 114, adoptado el 25 de noviembre del 2005. El supervisor europeo se mostró crítico con la amplitud de algunas de las excepciones, en su informe sobre el paquete de reforma.

- Consentimiento del interesado a la transferencia propuesta, tras haber sido informado de los riesgos, debido a la ausencia de garantías adecuadas.
- Transferencia necesaria para la ejecución de un contrato entre el interesado y responsable, o para la ejecución de medidas precontractuales a solicitud del interesado.
- Transferencia necesaria por razones de interés público. La Unión Europea o los estados miembros pueden establecer límites a la transferencia de categorías específicas de datos. Se notificarán a la Comisión.
- Transferencia necesaria para formular o defenderse de reclamaciones.
- Transferencia necesaria para proteger intereses vitales del interesado, cuando el interesado esté incapacitado para dar su consentimiento.
- Transferencia desde un registro público, abierto a la consulta pública de personas con interés legítimo. No abarcará la totalidad de los datos ni de las categorías, y solo se efectuará a solicitud de los destinatarios.
- Cuando no sea repetitiva, afecte a un número limitado de interesados y sea necesaria para el interés legítimo del interesado, o del responsable cuando no prevalezcan derechos del interesado, y el responsable considere que hay garantías. Se informará a la autoridad de control de la transferencia,

y se comunicarán al interesado los intereses legítimos imperiosos que han llevado a la transferencia.

Las novedades respecto a la Directiva son las siguientes (Piñar, 2016, págs. 454-456): en caso de consentimiento, este debe ser explícito, y no solo inequívoco; además, el interesado debe ser informado de los posibles riesgos (art. 49.1a RGPD); el interés público debe ser reconocido por el Derecho europeo o nacional (hay algunos ejemplos en el considerando 112); interés vital no solo del interesado, sino de otras personas, pero cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento (art. 49.1f RGPD); en el caso de transferencia desde un registro público, no abarcará todos los datos ni todas las categorías de datos, y si deben consultarla personas con interés legítimo, la transferencia solo se efectuará a solicitud de estas personas y si ellas son las destinatarias (art. 49.2 RGPD).

Por otro lado, ya hemos indicado que el WP29 prefería la adopción de cláusulas estándar antes que la referencia a una excepción del artículo 26 de la Directiva 95/46/CE, y la Comisión ha adoptado tres grupos de cláusulas estándar. Es de suponer que la misma posición se mantendrá con respecto al artículo 49 RGPD. Eso sí, existe también un documento del WP29 sobre la cooperación para el cumplimiento de las previsiones de protección de datos en las cláusulas contractuales del artículo 26.2 de la Directiva 95/46/CE[46].

(46)WP29, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Contractual clauses Considered as compliant with the EC Model Clauses*, adoptado el 26 de noviembre del 2014.

Bibliografía

AEPD (2016). *Códigos de conducta, certificaciones y transferencias internacionales* (8.ª sesión anual abierta).

Carpio, M. (2016). «Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 335-349). Madrid: Ed. Reus.

Cazurro, V. (2010). «Objeto y naturaleza de los códigos tipo». En: A. Troncoso (dir.). *Comentario a la Ley orgánica de protección de datos de carácter personal* (págs. 1747-1766). Cizur Menor: Civitas-Thomson Reuters.

Díaz-Romeral, A. (2016). «Los códigos de conducta en el Reglamento General de Protección de Datos». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 389-412). Madrid: Ed. Reus.

Fernández, C. M.; Recio, M. (2016). «Certificación en protección de datos personales». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 413-425). Madrid: Ed. Reus.

Kuchinke, W.; Krauth, C.; Bergmann, R.; Karakoyun, T.; Woollard, A.; Schluender, I.; Braasch, B.; Eckert, M.; Ohmann, C. (2016). «Legal assessment tool (LAT): an interactive tool to address privacy and data protection issues for data sharing». *Medical Informatics and Decision Making* (núm. 16, pág. 81).

Myers, A. (2016). «Cross-Border Commerce without constraint: Shifting from Territorial-Based Regulation to an Industry-Based Code of Conduct for the Online Payment Processing Industry». *The Computer & Internet Lawyer* (vol. 33, núm. 7, págs. 11-24).

Piñar, J. L. (2016). «Transferencias de datos personales a terceros países u organizaciones internacionales». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 427-460). Madrid: Ed. Reus.

Reichel, J. (2017). «Oversight of EU medical data transfers - an administrative law perspective on cross-border biomedical research administration». *Health Technol* (7 de marzo, págs. 1-12).

Remolina, N. (2015). *Tratamiento de información personal. Desde la transferencia transfronteriza hacia la recolección de datos personales: un reto del mundo post-Internet.* Premio de investigación AEPD del 2014. Madrid: Agencia Estatal Boletín Oficial del Estado / AEPD.

Rodotà, S. (2010). «Códigos de conducta: entre hard law y soft law». En: A. Real (coord.). *Códigos de conducta y actividad económica: una perspectiva jurídica*. Madrid: Marcial Pons.

Rubí, J. (2009). «Códigos tipo». En: R. Martínez (coord.). *Protección de datos. Comentarios al Reglamento de desarrollo de la LOPD* (págs. 167-199). Valencia: Tirant lo Blanch.